ABSTRACT

A method for identification includes the steps of generating system parameters, a private key and a public key, random numbers for obtaining an evidence, sending the evidence to a verifier by a prover, selecting a randomly selected number to obtain a query and sending the query R to the prover by the verifier, computing a temporary value to obtain a response and sending the response to the verifier by the prover, and determining a legitimacy of the prover by employing the system parameters, the public key, the evidence and the randomly selected number by the verifier. The method provides an identification scheme based on discrete logarithm problem, requiring no certificate and including only one query-and-response procedure.